

JV:AB
F. #2017R01691

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
TOMMYDAFNA@AOL.COM THAT IS
STORED AT PREMISES CONTROLLED
BY OATH, INC.

TO BE FILED UNDER SEAL

**APPLICATION FOR A
SEARCH WARRANT FOR
INFORMATION IN
POSSESSION OF A PROVIDER
(EMAIL ACCOUNT)**

Case No. 20-MJ-161

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jaclyn Nunez, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain email account, specifically "TOMMYDAFNA@aol.com" (the "SUBJECT EMAIL ACCOUNT"), that is stored at premises controlled by Oath, Inc. ("Oath"), an email provider headquartered at 22000 AOL Way, Dulles, Virginia 20166. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Oath to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Housing Finance Agency – Office of the Inspector General (“FHFA-OIG”) and have been so since January 2016. Since October 2017, I have been assigned to the El Dorado Task Force which consists of members from a number of law enforcement agencies, including the United States Department of Homeland Security, Homeland Security Investigations (“HSI”), and investigates financial crimes. As a Special Agent, I am responsible for investigating violations of, among other crimes, Title 18, United States Code, Sections 371 (conspiracy against the United States), 1343 (wire fraud), 1344 (bank fraud), 1349 (wire and bank fraud conspiracy), 1956 and 1957 (money laundering). During the course of these investigations, I have conducted or participated in surveillance and the execution of search warrants, used information gathered from tracking devices and reviewed electronic evidence. My experience also has included the investigation of the use of computers, cell phones and the internet to commit fraud. I have received training and have gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, computer evidence seizure and processing, and various other criminal law and procedures.

3. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The information contained in this affidavit includes information that I obtained from my personal participation in the investigation, reports made to me by other law enforcement agents and officers, information obtained from confidential sources of information, interviews with witnesses and from law enforcement and public records databases. The statements described in this affidavit are set forth in sum, substance, and in part.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 371, 1343, 1344, and 1349, and Title 18, United States Code, Sections 1956 and 1957, have been committed by Tomer Dafna, Iskyo Aronov, Michael Konstantinovskiy, Avraham Tarshish, Michael Herskowitz and others, known and unknown. There is also probable cause to search the information described in Attachment A for evidence, fruits and instrumentalities of these crimes, further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND

6. The Federal National Mortgage Association (“Fannie Mae”) and the Federal Home Loan Mortgage Corporation (“Freddie Mac”) are government-sponsored enterprises chartered by Congress. Fannie Mae and Freddie Mac purchase residential mortgage loans in the U.S. secondary market. The Federal Housing Finance Agency (“FHFA”) is a federal agency created on July 30, 2008 to oversee Fannie Mae, Freddie Mac, and the Federal Home Loan Banks. Fannie Mae and Freddie Mac are in conservatorships overseen by FHFA as conservator.

7. The United States Department of Housing and Urban Development (“HUD”) is a department of the Executive branch of the federal government. The Federal Housing Administration (“FHA”) is an agency of HUD. FHA provides mortgage insurance to

FHA-approved lenders who provided mortgages to borrowers that met certain eligibility requirements.

8. A pre-foreclosure sale, otherwise known as a “short sale,” allows a borrower who is in default on a mortgage loan to give up his or her property without a foreclosure. In a short sale, with the approval of the holder of a mortgage loan, referred to as “lender” herein, or the mortgage loan servicer, a borrower is permitted to sell his or her home for less than the outstanding balance of the mortgage. The proceeds from the short sale, minus approved closing costs, are applied to the outstanding mortgage balance owed to the lender, who typically agrees to forgive the borrower’s remaining mortgage balance.

9. HUD, Fannie Mae and Freddie Mac permit short sales of properties that secured loans they insure, guarantee or own if the short sale met certain requirements. Lenders and servicers typically require the parties to a proposed short sale to submit documents and information to show that the short sale meets the applicable requirements, or their own internal requirements for approving a short sale. Among other things, parties to a short sale typically are required to certify to the lender or servicer in an affidavit, sometimes referred to as a Short Sale Affidavit or an Arm’s Length Transaction Affidavit, that the sale is an arm’s length transaction and that: (1) there are no hidden terms or special understandings between any of the parties involved in the transaction; (2) any relationship or affiliation among the parties involved in the transaction has been disclosed to the lender or servicer; (3) neither the buyer nor the seller will receive any funds or commissions from the sale unless approved by the servicer or lender; (4) there are no current or pending higher offers, or contracts relating to the current sale or subsequent sale of the property that have not been disclosed to the lender or servicer; (5) all amounts paid to any person or entity in connection to the sale are approved and reflected on the

HUD-1 Settlement Statement; and (6) that the property has been listed for sale for a certain amount of time before any offers were evaluated and the presented offer yields the highest net return to the lender.

PROBABLE CAUSE

10. As described below, there is probable cause to believe that violations of Title 18, United States Code, Sections 371 (conspiracy against the United States), 1343 (wire fraud), 1344 (bank fraud), 1349 (wire and bank fraud conspiracy), 1956 and 1957 (money laundering), have been committed, and are being committed, by Tomer Dafna and others known and unknown. There is also probable cause to search the Devices described in Attachment A for evidence, instrumentalities, contraband and fruits of these crimes, further described in Attachment B.

A. The Short Sale Fraud Scheme

11. By way of background, the United States has been conducting a criminal investigation since 2017, into a short sale fraud scheme involving Dafna, Iskyo Aronov, also known as “Isaac Aronov,” Michael Konstantinovskiy, also known as “Michael Kay,” Avraham Tarshish, also known as “Avi Tarshish,” and Michael Herskowitz, among others, who conspired to defraud lenders, including lenders who held FHA-insured loans, Fannie Mae and Freddie Mac, and certain borrowers (collectively, the “Short Sale Victims”) by providing them with false, misleading and incomplete information to induce them to execute short sales of residential properties at fraudulently depressed prices, thereby causing losses to the lenders and, at times, the borrowers (the “Short Sale Scheme”). Dafna, Aronov, Konstantinovskiy, Tarshish and Herskowitz, and a number of other individuals, worked both together and separately to purchase hundreds of properties at fraudulently depressed prices and then resell or “flip” the properties for

large profits. In addition, I learned during the course of the investigation that Dafna owes the Internal Revenue Service large sums of money for past due unpaid taxes which he has claimed he is unable to pay.

12. The Short Sale Scheme originated at a company Aronov controlled known as My Ideal Property Inc. (“MIP”) located in Queens, New York, in late 2012, under the direction of Aronov. Aronov worked closely with Konstantinovskiy, who controlled National Homeowners Assistance Inc. (“NHA”), an entity that negotiated short sale approvals with servicers while purporting to represent the home owner. Tarshish initially worked under Aronov in 2013.

13. In the Short Sale Scheme, the Short Sale Co-Conspirators primarily targeted borrowers who owned homes in Brooklyn and Queens, New York, who were in default on their mortgages and in foreclosure proceedings. The Short Sale Co-Conspirators contacted borrowers who owned such properties and attempted to persuade the borrowers to sell their homes to the Short Sale Co-Conspirators in short sale transactions. If a borrower agreed, the Short Sale Co-Conspirators typically paid the borrower money to induce him or her also to sign: (1) an agreement with a real estate broker to list the property for sale, (2) an authorization to allow a third-party negotiator to negotiate the short sale with the lender on the borrower’s behalf and (3) a contract to sell the property to a corporate entity created for the purpose of acquiring the property and that was controlled by the Short Sale Co-Conspirators. These documents were typically sent to the lender or servicer. If a borrower contacted by the Short Sale Co-Conspirators agreed to participate in a short sale transaction, the Short Sale Co-Conspirators worked on obtaining access to and control over the property and monitored the progress of the short sale approval process.

14. Once a borrower agreed to sell his or her property in a short sale coordinated by the Short Sale Co-Conspirators, they did not market the property to other prospective buyers, regardless of any requirement to do so by the lender or servicer. Instead, they worked together to ensure that the Short Sale Co-Conspirators purchased the property for the lowest price that the lender or servicer would accept. The Short Sale Co-Conspirators typically instructed the broker who had listed the property for sale to tell any potential purchaser who inquired about the property that the property was already “under contract” or otherwise not available for a showing. The third-party negotiator, identified to the lender or servicer as the borrower’s agent and sometimes the same party who purportedly acted as the listing broker for the property, typically worked for the Short Sale Co-Conspirators and often was paid fees by the Short Sale Co-Conspirators in addition to and above any commission or fee disclosed to the lender or servicer. If a short sale offer was rejected by the lender or servicer, another corporate entity created by the Short Sale Co-Conspirators would submit another short sale offer after waiting for a period of time. The longer a property appeared to have been on the market, the greater the likelihood was that the lender or servicer would accept a proposed short sale price below any objective appraisal of the property’s value.

15. On occasion, the Short Sale Co-Conspirators paid a borrower money to transfer the deed of ownership of his or her property to a Short Sale Co-Conspirator before the Short Sale Co-Conspirators negotiated a short sale on behalf of the borrower with the lender or servicer. The deed transfer provided funds to the borrower, prevented the borrower from selling the property to another purchaser and gave the Short Sale Co-Conspirators control of the property even if the short sale was not approved. In instances involving such a deed transfer, certain borrowers were told only that they were agreeing to a short sale and did not understand

that they were, in fact, transferring their ownership rights to their property. Subsequently, prior to the closing of any approved short sale, the Short Sale Co-Conspirators transferred the deed back to the borrower for no consideration so that title of the property could be conveyed from the borrower to the short sale purchaser at the short sale closing in conformity with the terms of the sales contract signed by the borrower and provided to the lender or servicer as part of the short sale approval process.

16. The Short Sale Co-Conspirators also often filed fraudulent UCC-1 Financing Statements on properties the Short Sale Co-Conspirators intended to purchase so as to deter, or to obtain money from, other prospective buyers, who would need the filed UCC-1 Financing Statements terminated to clear the title of the property.

17. When the Short Sale Co-Conspirators submitted documentation to obtain approval for a short sale, they provided false, misleading and incomplete information to the lender or servicer. Among other things, in the required short sale affidavit and transaction documents, the Short Sale Co-Conspirators did not disclose that payments had been made to the borrower, that the property was not marketed as required and that the agents for the borrower and purchaser were affiliated by commercial enterprise. Furthermore, the Short Sale Co-Conspirators did not disclose all the past and future payments, including fees and commissions, to be paid to the Short Sale Co-Conspirators or the borrower in connection with the short sale.

18. In or about January 2014, Dafna and Tarshish replicated the Short Sale Scheme at companies they created known as Exclusive Homes Realty Group Inc., Exclusive Homes NY, LLC (together, "Exclusive Homes") and Homeowners Solutions Group LTD ("Homeowners Solutions") all located in Brooklyn, New York. Herskowitz was a real estate attorney who assisted Aronov and Dafna in completing certain fraudulent short sale transactions.

B. Dafna's Role

19. Dafna, together with Tarshish, owned Exclusive Homes Realty Group, Inc., and multiple other business entities through which he purchased and sold properties involved in the Short Sale Scheme. In his capacity as owner, and sometimes corporate officer, of these entities, Dafna would – through his subordinates – arrange for the purchase of properties in short sales, negotiating the purchase price, communicating with the banks that held the mortgages on the properties prior to purchase and arranging for undisclosed side payments to the property-owners. In short, Dafna, together with Tarshish, would control and direct the transactions under investigation.

20. While Exclusive Homes and most of the corporate entities formed to acquire specific properties acquired in short sales by Dafna were nominally owned by others, multiple individuals who were interviewed by agents prior to April 2019, identified Dafna as an owner of Exclusive Homes and involved in the Short Sale Scheme. In addition, on or about January 20, 2017, Dafna signed an affidavit in a civil lawsuit against a property owner and a former employee of Exclusive Homes. In the affidavit, DAFA identified himself as the “owner of Exclusive Homes Realty Group, Inc.” Exclusive Homes Realty Group, Inc., et al. v. Carillo and Torres, Sup. Ct. Kings Cnty, No. 502118/2017. Dafna also stated in the affidavit that while a former employee of Exclusive Homes “formed [corporate] entities using her name and signature as part of Exclusive Homes Realty’s Group’s business practice, to facilitate the purchase of different properties[, said] entities are formed, operated, managed exclusively by Exclusive Homes Realty Group, and they are not owned by the individual agent or broker, but by Exclusive Homes Realty Group, Inc.”

21. A Short Sale Co-Conspirator (“Short Sale Co-Conspirator 1”), [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] [REDACTED]

[REDACTED] worked for Aronov and Tarshish at MIP, and then worked with Dafna and Tarshish at Exclusive Homes. [REDACTED]

[REDACTED]

Among other things, Short Sale Co-Conspirator 1 directly approached homeowners and persuaded them to sell their properties in short sales coordinated by MIP or Exclusive Homes. Short Sale Co-Conspirator 1 also filed hundreds of fraudulent UCC-1 Financing Statements on properties that Exclusive Homes wanted to purchase to try to ensure that Exclusive Homes and Short Sale Co-Conspirator 1 would get paid money if another party ended up purchasing the property.

[REDACTED]

[REDACTED]

23. Agents have identified a number of fraudulent short sale transactions that involved Dafna, including the short sales of the properties at 177 Lewis Avenue, Brooklyn, New York (“177 Lewis Avenue”), and 65 Glen Street Brooklyn, New York (“65 Glen Street”). In both of these transactions, after the servicer approved the short sale to a specific corporate entity controlled by Dafna and his co-conspirators at a specific price but before the transaction closed, Dafna and others secretly arranged to sell the property for amounts above the short sale price by transferring the corporate entity to a subsequent purchaser at or about the time of the closing. For example, the servicer agreed to a short sale of 177 Lewis Avenue for a price of \$275,000 to an entity controlled by Dafna on or about April 30, 2015, but, as indicated by an email sent by Short Sale Co-Conspirator 1 referenced in paragraph 24 below, the price secretly paid by the subsequent purchaser was over \$700,000. With respect to 65 Glen Street the servicer agreed to a short sale of this property at a price of \$200,000 on or about March 15, 2018, but the price secretly paid by the subsequent purchaser was at least a couple of hundred thousand dollars more according to Short Sale Co-Conspirator 1. Public records indicate that on or about March 15, 2018, the corporate entity that acquired 65 Glen Street took out mortgage for \$525,000 secured by the property. Both of these transactions involved fraudulent representations by the Short Sale Co-Conspirators to the servicer who approved the sale. These included false statements about the true nature of the transaction, the actual purchase price paid, and the payments made to the various parties involved in the transactions.

24. The following emails related to the 177 Lewis Avenue short sale:

a. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

b. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

c. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

d. On or about April 28, 2015, Dafna emailed several individuals regarding the corporation which would be purchasing 177 Lewis Avenue. Dafna's email was sent from the SUBJECT EMAIL ACCOUNT.

e. On or about April 29, 2015, Dafna emailed several individuals that he would attend the short sale closing for the 177 Lewis Avenue transaction [REDACTED]

[REDACTED]. Dafna's email was sent from the SUBJECT EMAIL ACCOUNT.

f. On May 18, 2015, after the 177 Lewis Avenue short sale had occurred, [REDACTED]

[REDACTED] the actual, secretly arranged, purchase

price for 177 Lewis Avenue was \$775,000, the total costs were \$436,200, including \$20,000 paid for the "Deed," the profit on this transaction was \$338,800, [REDACTED]

[REDACTED]

25. The following emails related to the 65 Glen Street short sale:

a. [REDACTED]

[REDACTED]

[REDACTED]

b. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

c. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

d. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

26. [REDACTED]

[REDACTED]

27.

28. During the course of the investigation, I reviewed bank records of accounts controlled by numerous individuals, including Dafna and Herskowitz. I determined that Dafna generally does not hold many assets in his own name but often moves money between accounts controlled by others, which appears to be an effort to disguise the source or ownership of the funds. For example, agents identified over \$30,000,000 in monetary transactions

associated with Dafna that were conducted through Herskowitz's Interest on Lawyer Trust Account ("IOLA") between 2014 and March 2017, including numerous wire transfers to and from Israel and China.

29. During the course of the investigation, on or about January 30, 2019, I interviewed Herskowitz,² who stated, among other things and in sum and substance, that prior to Herskowitz's arrest in March of 2017 by the Queens District Attorney's Office for his involvement in an unrelated deed fraud case, Herskowitz represented Dafna and Tarshish in hundreds of real estate transactions in the New York area between 2014 and March 2017. Among other things that he did for Dafna and Tarshish, Herskowitz stated he sent money through his IOLA account to consummate short sale transactions. Herskowitz also stated that, in or about 2015, Dafna opened the Whitestone Asset Group, Inc., and this company was supposed to get investors in Israel to invest money in short sales in New York City.

30. In general, an email that is sent to an Oath subscriber is stored in the subscriber's "mail box" on Oath's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Oath's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Oath's servers for a certain period of time.

² Herskowitz retracted certain statements he made during this interview at a later date. Those statements are not described herein. While agents believe that Herskowitz's statements included in this Affidavit are accurate, and they are corroborated by other sources of information, agents assess that Herskowitz was not truthful when asked about his participation in the Short Sale Scheme, as he primarily denied any involvement in fraud.

31. On August 23, 2019, the Honorable Steven M. Gold, United States Magistrate Judge for the Eastern District of New York, issued a Search and Seizure Warrant for forensic images of two iPhones and an iPad which were in Dafna's possession during the course of a border inspection (19-MJ-765) (Under Seal). The returns from that Search and Seizure Warrant were not included or used, in whole or in part, as a basis for this Application.

32. On September 6, 2019, a Grand Jury returned an indictment against Dafna, Aronov, Konstantinovsky, Tarshish and Herskowitz, charging violations of Title 18, United States Code, Sections 1343 and 1349.

33. On September 9, 2019, the Honorable Lois Bloom, United States Magistrate Judge for the Eastern District of New York issued a search warrant for Dafna's home, for the Premises Known and Described as 9 Stream Court, Great Neck, New York, 11023 (19-MJ-806) (Under Seal). The returns from that Search and Seizure Warrant were not included or used, in whole or in part, as a basis for this Application.

34. On August 14, 2019, the government served a preservation request pursuant to 18 U.S.C. § 2703(f) upon Oath and renewed that request pursuant to 18 U.S.C. § 2703(f)(2) on November 14, 2019. Both requests asked Oath to preserve all stored communications, records and other evidence regarding the SUBJECT EMAIL ACCOUNT for a period of 90 days.

C. Indictment

35. On September 6, 2019, a Grand Jury returned an indictment against Tomer Dafna, Iskyo Aronov, Michael Konstantinovskiy, Avraham Tarshish and Michael Herskowitz. See United States v. Aronov, et al., 19-CR-408 (MKB). The United States' investigation into the

conduct underlying the allegations in the indictment and into additional charges against the defendants and others, known and unknown, is ongoing.

BACKGROUND CONCERNING EMAIL

36. In my training and experience, I have learned that Oath provides a variety of on-line services, including electronic mail ("email") access, to the public. Oath allows subscribers to obtain email accounts at the domain name aol.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Oath. During the registration process, Oath asks subscribers to provide basic personal information. Therefore, the computers of Oath are likely to contain stored electronic communications (including retrieved and unretrieved email for Oath subscribers) and information concerning subscribers and their use of Oath services, such as account access information, email transaction information and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

37. An Oath subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Oath. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

38. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone

numbers and other identifiers, alternative email addresses and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

39. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

40. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute

evidence of the crimes under investigation because the information can be used to identify the account's user or users.

41. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or

consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

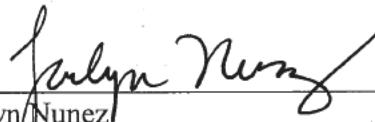
42. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Oath, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING AND NON-DISCLOSURE

43. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation. The scope of the ongoing criminal investigation is not public nor known to all of the targets of the investigation. Specifically, even though certain participants in the Short Sale Scheme have been arrested, the government is investigating and may seek to indict additional participants, who should they learn of the scope of our investigation, may attempt to flee from prosecution, destroy or tamper with evidence, change patterns of behavior, intimidate potential witnesses, notify confederates or otherwise seriously jeopardize the investigation. Moreover, some of the evidence in this investigation involves communications that can be transferred to alternate platforms (including encrypted platforms and platforms beyond the jurisdictional reach of U.S. legal process). If alerted to the existence of the warrant and the broader scope of the ongoing investigation, there is reason to believe that the subjects under investigation may seek to destroy that evidence and change their patterns of behavior. Accordingly, there is good cause to seal all papers in support of this application.

44. Pursuant to 18 U.S.C. § 2705(b) and for the reasons stated above, it is further requested that the Court issue an Order commanding Oath not to notify any person (including subscribers or customers of the account listed in the attached warrant) of the existence of the attached warrant for the period of one year from the date of the Order, except that Oath may disclose the warrant to its respective attorney for the purpose of receiving legal advice.

Respectfully submitted,


Jaclyn Nunez
Special Agent
FHFA-OIG

Subscribed and sworn to before me on February 14, 2020



s/Lois Bloom


HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with "TOMMYDAFNA@aol.com" that is stored at premises owned, maintained, controlled or operated by Oath, Inc., a company headquartered at 22000 AOL Way, Dulles, Virginia 20166.

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by Oath, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on August 14, 2019, and renewed pursuant to 18 U.S.C. § 2703(f)(2) on November 14, 2019, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken. The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be Seized by the Government

All information described above in Section I that evidence, fruits and instrumentalities of wire fraud, bank fraud, and conspiracy to commit wire fraud and bank fraud, in violation of Title 18, United States Code, Sections 371, 1343, 1344, and 1349, and money laundering, in violation of Title 18, United States Code, Sections 1956 and 1957, involving Tomer Dafna and occurring after January 1, 2014, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) All records and information described in Attachment A, including names and telephone numbers, as well as the contents of all call logs, contact lists, text messages, emails (including those sent, received, deleted and drafted), instant messages, photographs, videos, Facebook posts, Internet activity (including browser history, web page logs, and search terms entered by the user), and other electronic media constituting evidence, fruits or instrumentalities of a conspiracy to wire fraud, bank fraud, and conspiracy to commit wire fraud and bank fraud, in violation of Title 18, United States Code, Sections 371, 1343, 1344, and 1349, and money laundering, in violation of Title 18, United States Code, Sections 1956 and 1957;
- (b) any information related to real estate transactions involving fraudulent short sales or misrepresentations to mortgage loan lenders or servicers;

- (c) any information related to the disposition of proceeds obtained from fraudulent short sales transactions;
- (d) any communications among the participants in the scheme to engage in fraudulent short sale transactions;
- (e) all bank records, checks, credit card bills, account information, and other financial records;
- (f) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (g) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation; and
- (h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (i) Records relating to the identity of, and email accounts used by, persons and business that communicated with the email account owner concerning real estate transactions involving fraudulent short sales or misrepresentations to mortgage loan lenders or servicers, including records that help reveal their whereabouts.